Sub B2

WHAT IS CLAIMED IS:

1. A system comprising:

a computer bus;

a host processor connected to the computer bus, the host processor being programmed to perform error code correction;

a drive including means for providing a block of ECC-encoded data; means for providing an encryption mask; means for performing a bitwise XOR of the encryption mask and the block of ECC-encoded data, a product of the bitwise XOR being an encrypted block, an output of the bitwise XOR means being coupled to the computer bus, whereby the encrypted block can be sent to the host processor via the computer bus for error code correction.

2. The system of claim 1, wherein the means for providing the encryption mask includes means for providing a seed, a pseudorandom data generator for generating a sequence of random numbers from the seed, and an ECC encoder for generating an encryption mask including first and second portions, the first portion including the random numbers, the second portion including redundancy data for the first portion.

3. The system of claim 2, further comprising means, coupled to the computer bus, for receiving the encrypted block from the host processor; means for receiving the seed from the drive; a second pseudorandom generator for generating a decryption mask from the seed; means for performing a second bitwise XOR of the decryption mask and user data in the encrypted block, a product of the second bitwise XOR providing unencrypted user data.

4. The system of claim 3, further comprising an MPEG decoder coupled to an output of the means for performing the second bitwise XOR.

5. The system of claim 4, wherein the drive is a DVD-ROM drive, and wherein a DVD decoder card includes the MPEG decoder, the means for receiving the encrypted block, the means for receiving the seed; the second pseudorandom generator and the means for performing the second bitwise XOR.

6. The system of claim 1, wherein the ECC block includes a first portion for user data and a second portion for redundancy data, and wherein the encryption mask includes third and fourth portions corresponding to the first and second portions, respectively, of the ECC block.

7. The system of claim 6, wherein the third portion is filled with a plurality of numbers, and wherein the fourth portion includes redundancy data generated from the third portion.

8. The system of claim 6, wherein the third portion is filled selectively with a plurality of numbers, and wherein the fourth portion includes redundancy data generated from the third portion.

9. The system of claim 1, wherein the ECC block is coded according to an error code correction method, and wherein the encryption mask is coded according to the same error code correction method.

B2

10. The system of claim 1, wherein the drive further includes means for performing error code correction, and wherein the host processor also performs error code correction on the encrypted data sent by the drive.

11. A drive comprising:

means for reading an ECC block from a storage medium;

means for providing a seed;

a pseudorandom data generator for generating a sequence of random numbers from the seed;

means for generating an encryption mask including a sequence of random numbers and redundancy data, the random numbers being generated from the seed; and

means for performing a bitwise XOR of the encryption mask and the ECC block, a product of the bitwise XOR being an encrypted ECC block.

12. The drive of claim 11, wherein the ECC block includes a first portion for user data and a second portion for redundancy data, and wherein the encryption mask includes a third and fourth portions corresponding to the first and second portions, respectively, of the ECC block.

13. The drive of claim 12, wherein the third portion is filled entirely with random numbers, and wherein the fourth portion includes redundancy data generated from the third portion.

14. The drive of claim 12, wherein the third portion is filled selectively with random numbers and zeros, and wherein the fourth portion includes redundancy data generated from the third portion.

15. The drive of claim 11, wherein the ECC block is coded according to an error code correction method, and wherein the encryption mask is coded according to the same error code correction method.

16. The drive of claim 11, further comprising means for performing error code correction on the ECC block.

17. A method of transmitting secured data over a bus, the method comprising:

receiving an ECC block;

generating an encryption mask including a plurality of numbers and redundancy data;

performing a bitwise XOR of the encryption mask and the ECC block, a product of the bitwise XOR being an encrypted ECC block; and

sending the encrypted ECC block over the bus.

18. The method of claim 17, further comprising the step of using the host processor to perform error code correction on the encrypted block.

19. The method of claim 17, further comprising the step of performing partial error-correction on the ECC block before performing the bitwise XOR and sending the encrypted block sent over the bus.

20. The method of claim 17, wherein the ECC block includes a first portion for user data and a second portion for redundancy data, and wherein the step of generating the encryption mask includes the steps of filling a first portion of the encryption mask entirely with random numbers, and filling a second portion of the encryption mask with redundancy data for the first portion, the first and second portions of the encryption mask corresponding to the first and second portions of the ECC block.

21. The method of claim 17, wherein the ECC block includes a first portion for user data and a second portion for redundancy data, and wherein the step of generating the encryption mask includes the steps of filling a first portion of

the encryption mask selectively with numbers and zeros, and filling a second portion of the encryption mask with redundancy data generated from the numbers, the first and second portions of the encryption mask corresponding to the first and second portions of the ECC block.

22. The method of claim 17, further comprising the step of decrypting the encrypted block, the step of decrypting including generating a decryption mask; and performing a bitwise XOR of the decryption mask and user data in the encrypted ECC block, a product of the bitwise XOR providing unencrypted user data.

a

23. The method of claim 22, wherein the encryption mask is generated during encryption via a seed and a random number generator algorithm, and wherein the decryption mask is generated during decryption by using the same seed and the same random number generator algorithm.

24. The method of claim 17, further comprising the step of regenerating the encrypted block for subsequent data transmission.

25. The method of claim 17, further comprising the step of reusing the random data block for encryption of subsequent data blocks.

Add a2